HOUSE BILL No. 1357

DIGEST OF INTRODUCED BILL

Citations Affected: IC 4-6-14-3; IC 24-4-14-6; IC 24-4.9.

Synopsis: Data breaches. Makes the following changes to the statute concerning the breach of the security of data that includes the sensitive personal information of Indiana residents and that is collected and maintained by a person other than a state agency or the judicial or legislative department of state government: (1) Specifies that the statute is not limited to breaches of computerized data. (2) Repeals the definition of a term ("doing business in Indiana") that is not used in the statute. (3) Replaces the term "data base owner" with "data owner". (4) Defines the term "data collector" as a person that: (A) is not a data owner; and (B) collects, maintains, disseminates, or handles data that includes sensitive personal information. (5) Defines the term "data user" as a data owner or a data collector. (6) Replaces the term "personal information" with "sensitive personal information" and makes conforming amendments. (7) Requires a data user to post certain information concerning the data user's privacy practices on the data user's Internet web site. (8) Increases the amount of the civil penalty that a court may impose in an action by the attorney general to enforce the provisions concerning the safeguarding of data if the court finds that a violation: (A) was done knowingly; or (B) contributed to a breach of the security of data that includes the sensitive personal information of Indiana residents. (9) Sets forth certain information that a data owner must include in a disclosure of a security breach. (10) Specifies the applicability of different enforcement procedures available to the attorney general under the statute.

Effective: July 1, 2016.

Fine

January 12, 2016, read first time and referred to Committee on Utilities, Energy and Telecommunications.

Introduced

Second Regular Session of the 119th General Assembly (2016)

PRINTING CODE. Amendments: Whenever an existing statute (or a section of the Indiana Constitution) is being amended, the text of the existing provision will appear in this style type, additions will appear in **this style type**, and deletions will appear in ~~this style type.~~

Additions: Whenever a new statutory provision is being enacted (or a new constitutional provision adopted), the text of the new provision will appear in **this style type**. Also, the word **NEW** will appear in that style type in the introductory clause of each SECTION that adds a new provision to the Indiana Code or the Indiana Constitution.

Conflict reconciliation: Text in a statute in *this style type* or ~~*this style type*~~ reconciles conflicts between statutes enacted by the 2015 Regular Session of the General Assembly.

HOUSE BILL No. 1357

A BILL FOR AN ACT to amend the Indiana Code concerning trade regulation.

Be it enacted by the General Assembly of the State of Indiana:

SECTION 1. IC 4-6-14-3, AS ADDED BY P.L.84-2010, SECTION 1, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 3. As used in this chapter, "personal information" ~~has the meaning set forth in IC 24-4.9-2-10.~~ **means:**

(1) a Social Security number that is not encrypted or redacted; or

(2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:

(A) A driver's license number.

(B) A state identification card number.

(C) A credit card number.

(D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local

government records lawfully made available to the general public.

SECTION 2. IC 24-4-14-6, AS ADDED BY P.L.125-2006, SECTION 5, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 6. **(a)** As used in this chapter, "personal information" ~~has the meaning set forth in IC 24-4.9-2-10.~~ **means:**

(1) a Social Security number that is not encrypted or redacted; or

(2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:

(A) A driver's license number.

(B) A state identification card number.

(C) A credit card number.

(D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

The term includes information stored in a digital format.

(b) The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

SECTION 3. IC 24-4.9-2-2, AS AMENDED BY P.L.137-2009, SECTION 3, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 2. (a) "Breach of the security of data" means unauthorized acquisition of ~~computerized~~ data that compromises the security, confidentiality, or integrity of **sensitive** personal information maintained by a ~~person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.~~ **data user.**

(b) The term does not include the following:

(1) Good faith acquisition of **sensitive** personal information by an employee or agent of the ~~person~~ **data user** for lawful purposes of the ~~person,~~ **data user,** if the **sensitive** personal information is not used **for unlawful purposes** or subject to further unauthorized disclosure.

(2) Unauthorized acquisition of a portable electronic device on which **sensitive** personal information is stored, if all **sensitive** personal information on the device is protected by encryption and the encryption key:

(A) has not been compromised or disclosed; and

(B) is not in the possession of or known to the person who,

without authorization, acquired or has access to the portable electronic device.

SECTION 4. IC 24-4.9-2-2.7 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: **Sec. 2.7. "Data" means electronic or printed information that is collected, maintained, disseminated, or handled:**

(1) in a computerized format;

(2) on paper;

(3) on microfilm; or

(4) in another medium.

SECTION 5. IC 24-4.9-2-2.8 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: **Sec. 2.8. "Data collector" means a person that:**

(1) is not a data owner; and

(2) collects, maintains, disseminates, or handles data that includes the sensitive personal information of an Indiana resident.

SECTION 6. IC 24-4.9-2-3, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 3. "Data ~~base~~ owner" means a person that owns or licenses ~~computerized~~ data that includes **the sensitive** personal information **of an Indiana resident.**

SECTION 7. IC 24-4.9-2-3.2 IS ADDED TO THE INDIANA CODE AS A **NEW** SECTION TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: **Sec. 3.2. "Data user" means a:**

(1) data owner; or

(2) data collector.

SECTION 8. IC 24-4.9-2-4 IS REPEALED [EFFECTIVE JULY 1, 2016]. ~~Sec. 4. "Doing business in Indiana" means owning or using the personal information of an Indiana resident for commercial purposes.~~

SECTION 9. IC 24-4.9-2-7, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 7. "Indiana resident" means a person whose principal mailing address is in Indiana, as reflected in records maintained by ~~the~~ **a** data ~~base owner.~~ **user.**

SECTION 10. IC 24-4.9-2-10, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 10. ~~"Personal~~ **"Sensitive personal** information" means:

(1) a Social Security number that is not encrypted or redacted; or

(2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:

(A) A driver's license number.

(B) A state identification card number.

(C) A credit card number.

(D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

SECTION 11. IC 24-4.9-2-11, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 11. (a) Data are redacted for purposes of this article if the data have been altered or truncated so that not more than the last four (4) digits of:

(1) a driver's license number;

(2) a state identification number; or

(3) an account number;

is accessible as part of **sensitive** personal information.

(b) For purposes of this article, **sensitive** personal information is "redacted" if the **sensitive** personal information has been altered or truncated so that not more than five (5) digits of a Social Security number are accessible as part of **the sensitive** personal information.

SECTION 12. IC 24-4.9-3-1, AS AMENDED BY P.L.137-2009, SECTION 4, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 1. (a) Except as provided in section ~~4(c), 4(d), and~~ 4(e), **4(f), and 4(g)** of this chapter, after discovering or being notified of a breach of the security of data, ~~the~~ **a** data ~~base~~ owner shall disclose the breach to an Indiana resident whose:

(1) unencrypted **sensitive** personal information was or may have been **accessed or** acquired by an unauthorized person; or

(2) encrypted **sensitive** personal information was or may have been **accessed or** acquired by an unauthorized person with access to the encryption key;

if the data ~~base~~ owner knows, should know, or should have known that the unauthorized **access or** acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.

(b) A data ~~base~~ owner required to make a disclosure under subsection (a) to more than one thousand (1,000) ~~consumers~~ **Indiana**

residents shall also disclose to each consumer reporting agency **that compiles and maintains files on consumers on a nationwide basis** (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including **fraud involving the sensitive** personal information of an Indiana resident affected by the breach of the security of a system.

(c) If a data ~~base~~ owner makes a disclosure described in subsection (a), the data ~~base~~ owner shall also disclose the breach to the attorney general.

SECTION 13. IC 24-4.9-3-2, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 2. A ~~person~~ **data collector** that maintains ~~computerized~~ data ~~but that is not a data base owner~~ shall notify the data ~~base~~ owner if the ~~person~~ **data collector** discovers that **sensitive** personal information was or may have been acquired by an unauthorized person.

SECTION 14. IC 24-4.9-3-3, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 3. (a) A ~~person~~ **data user** required to make a disclosure or notification under this chapter shall make the disclosure or notification without unreasonable delay. For purposes of this section, a delay is reasonable if the delay is:

(1) necessary to restore the integrity of ~~the~~ **a** computer system;

(2) necessary to discover the scope of the breach; or

(3) in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will:

(A) impede a criminal or civil investigation; or

(B) jeopardize national security.

(b) A ~~person~~ **data user** required to make a disclosure or notification under this chapter shall make the disclosure or notification as soon as possible after:

(1) delay is no longer necessary to restore the integrity of ~~the~~ **a** computer system or to discover the scope of the breach; or

(2) the attorney general or a law enforcement agency notifies the ~~person~~ **data user** that ~~delay~~ **disclosure** will no longer impede a criminal or civil investigation or jeopardize national security.

SECTION 15. IC 24-4.9-3-3.5, AS ADDED BY P.L.137-2009, SECTION 5, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 3.5. (a) This section does not apply to a data ~~base owner~~ **user** that ~~maintains~~ **is required to maintain** its own data security procedures, **and maintains such procedures,** as part of an information privacy, security policy, or compliance plan under:

(1) the federal USA PATRIOT Act (P.L. 107-56);
(2) Executive Order 13224;
(3) the federal Driver's Privacy Protection Act (18 U.S.C. 2721 et seq.);
(4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(5) the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or
(6) the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191), **as amended by the federal Health Information Technology for Economic and Clinical Health (HITECH) Act (P.L. 111-5);**

if the data ~~base owner's~~ **user's** information privacy, security policy, or compliance plan requires the data ~~base owner~~ **user** to maintain reasonable procedures to protect and safeguard from unlawful use or disclosure **sensitive** personal information of Indiana residents that is collected or maintained by the data ~~base owner~~ **user** and the data ~~base owner~~ **user** complies with the data ~~base owner's~~ **user's** information privacy, security policy, or compliance plan.

(b) A data ~~base owner~~ **user** shall:

(1) subject to subsection (c), implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any **data that includes the sensitive** personal information of Indiana residents **and that is** collected or maintained by the data ~~base owner.~~ **user; and**

(2) conspicuously post on the Internet web site, if any:

(A) that is publicly accessible; and

(B) through which data that includes the sensitive personal information of Indiana residents is collected;

the data user's privacy policy with respect to sensitive personal information collected through the Internet web site and maintained by the data user.

(c) Procedures implemented and maintained by a data user under subsection (b)(1) must require that the data user:

(1) retain sensitive personal information only as reasonably necessary for:

(A) a legitimate business, governmental, academic, or nonprofit purpose; or

(B) compliance with applicable law;

(2) not use sensitive personal information in contravention of law; and

(3) not use sensitive personal information unless:

(A) the use is reasonably necessary for a legitimate business, governmental, academic, or nonprofit purpose; and

(B) the individual to whom the sensitive personal information relates has not previously communicated to the data user that such use is not authorized by the individual.

~~(c)~~ **(d)** A data ~~base owner~~ **user** shall not dispose of records or documents containing unencrypted ~~and~~ **or** unredacted **sensitive** personal information of Indiana residents without shredding, incinerating, mutilating, erasing, or otherwise rendering the **sensitive** personal information illegible or unusable.

(e) A data user shall not:

(1) make a misrepresentation to an Indiana resident concerning the data user's collection, storage, use, sharing, or destruction of sensitive personal information; or

(2) require a vendor or contractor to make a misrepresentation described in subdivision (1).

~~(d)~~ **(f)** A person that ~~knowingly or intentionally~~ fails to comply with ~~any provision of~~ this section commits a deceptive act that is actionable only by the attorney general under this section. **A person that fails to comply with section 1, 2, 3, or 4 of this chapter commits a deceptive act that is actionable only by the attorney general under IC 24-4.9-4. The enforcement procedures available under this section are cumulative and an enforcement procedure available under this section is supplemental to any other enforcement procedure available under:**

(1) this section;

(2) IC 24-4.9-4; or

(3) any other law, rule, or regulation of this state;

for a violation of this article.

~~(e)~~ **(g)** The attorney general may bring an action under this section to obtain any or all of the following:

(1) An injunction to enjoin further violations of this section.

(2) **Subject to subsections (i) and (j),** a civil penalty of not more than ~~five~~ **one** thousand dollars ~~($5,000)~~ **($1,000)** per deceptive act.

(3) The attorney general's reasonable costs in:

(A) the investigation of the deceptive act; and

(B) maintaining the action.

~~(f)~~ **(h) Subject to subsection (i),** a failure to comply with subsection (b) or ~~(c)~~ **(d)** in connection with related acts or omissions constitutes

one (1) deceptive act.

(i) Subject to subsection (j), in an action brought under this section, if the court determines that a failure to comply with this section was done knowingly, the court may impose a civil penalty of not more than the greater of:

(1) five thousand dollars ($5,000); or

(2) fifty dollars ($50) for each affected Indiana resident if the failure to comply contributed to a breach of the security of data.

(j) The total civil penalties imposed under subsection (g) or (i) in connection with one (1) deceptive act may not exceed one hundred fifty thousand dollars ($150,000).

(k) The consumer protection division of the office of the attorney general shall use civil penalties collected under this article to enforce this article.

SECTION 16. IC 24-4.9-3-4, AS AMENDED BY P.L.137-2009, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 4. (a) Except as provided in subsection ~~(b),~~ **(c),** a data ~~base~~ owner required to make a disclosure under **section 1 of** this chapter shall make the disclosure using one (1) of the following methods:

(1) Mail.

(2) Telephone.

(3) Facsimile (fax).

(4) Electronic mail, if the data ~~base~~ owner has the electronic mail address of the affected Indiana resident.

(b) A disclosure under section 1 of this chapter must include the following:

(1) A description of the breach of the security of data in general terms.

(2) A description of the sensitive personal information that was subject to unauthorized access or acquisition.

(3) A general description of any actions by the data owner to protect the sensitive personal information from further unauthorized access.

(4) The toll free telephone numbers and addresses for the consumer reporting agencies described in section 1(b) of this chapter.

(5) The toll free telephone numbers, addresses, and Internet web site addresses for the Federal Trade Commission and the office of the attorney general, along with a statement that an individual may obtain from the Federal Trade Commission

and the office of the attorney general information about preventing identity theft.

~~(b)~~ **(c)** If a data ~~base~~ owner **is** required to make a disclosure under **section 1 of** this chapter ~~is required to make~~ **and:**

(1) the disclosure **must be made** to more than five hundred thousand (500,000) Indiana residents; ~~or if the data base owner required to make a disclosure under this chapter determines that~~

(2) the **associated** cost of the disclosure will be more than two hundred fifty thousand dollars ($250,000); **or**

(3) the data ~~base~~ owner ~~required to make a disclosure under this chapter~~ **does not have sufficient contact information for Indiana residents to make the required disclosure;**

the data owner may elect to make the disclosure by using both of the ~~following~~ methods **set forth in subsection (d), as an alternative to the methods set forth in subsection (a).**

(d) A data owner described in subsection (c) may elect to make the disclosure required under section 1 of this chapter using both of the following methods, as an alternative to the methods set forth in subsection (a):

(1) ~~Conspicuous~~ **Conspicuously** posting ~~of the notice~~ on the **data owner's Internet** web site, ~~of the data base owner, if the data base owner maintains a web site.~~ **if any, a notice of the breach of the security of data.**

(2) **Providing** notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of ~~a system~~ **the data** reside.

~~(c)~~ **(e)** A data ~~base~~ owner that maintains its own disclosure procedures as part of an information privacy policy or a security policy is not required to make a separate disclosure under **section 1 of** this chapter if the data ~~base~~ owner's information privacy policy or security policy is at least as stringent as the disclosure requirements described in:

(1) sections 1 through ~~4(b)~~ **4(d)** of this chapter;

(2) subsection ~~(d);~~ **(f);** or

(3) subsection ~~(c).~~ **(g).**

~~(d)~~ **(f)** A data ~~base~~ owner that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under:

(1) the federal USA PATRIOT Act (P.L. 107-56);

(2) Executive Order 13224;

(3) the federal Driver's Privacy Protection Act (18 U.S.C. 2781 et seq.);

(4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(5) the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or

(6) the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191), **as amended by the federal Health Information Technology for Economic and Clinical Health (HITECH) Act (P.L. 111-5);**

is not required to make a disclosure under **section 1 of** this chapter if the data ~~base~~ owner's information privacy, security policy, or compliance plan requires that Indiana residents be notified of a breach of the security of data without unreasonable delay and the data ~~base~~ owner complies with the data ~~base~~ owner's information privacy, security policy, or compliance plan.

~~(e)~~ **(g)** A financial institution that complies with the disclosure requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, as applicable, is not required to make a disclosure under this chapter.

~~(f)~~ **(h)** A person required to make a disclosure under this chapter may elect to make all or part of the disclosure in accordance with subsection (a) even if the person could make the disclosure in accordance with subsection ~~(b).~~ **(d).**

SECTION 17. IC 24-4.9-4-1, AS AMENDED BY P.L.137-2009, SECTION 7, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 1. (a) A person that is required to make a disclosure or notification in accordance with IC 24-4.9-3 and that fails to comply with any provision of this article, **other than IC 24-4.9-3-3.5,** commits a deceptive act that is actionable only by the attorney general under this chapter. **A person that fails to comply with IC 24-4.9-3-3.5 commits a deceptive act that is actionable only by the attorney general under IC 24-4.9-3-3.5. The enforcement procedures available under this chapter are cumulative, and an enforcement procedure available under this chapter is supplemental to any other enforcement procedure available under:**

(1) this chapter;

(2) IC 24-4.9-3-3.5; or

(3) any other law, rule, or regulation of this state;

for a violation of this article.

(b) A failure to make a required disclosure or notification in connection with a related series of breaches of the security of data constitutes one (1) deceptive act.

SECTION 18. IC 24-4.9-4-2, AS ADDED BY P.L.125-2006, SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2016]: Sec. 2. **(a)** The attorney general may bring an action under this chapter to obtain any or all of the following:

(1) An injunction to enjoin future violations of IC 24-4.9-3, **other than a violation of IC 24-4.9-3-3.5.**

(2) A civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act.

(3) The attorney general's reasonable costs in:

(A) the investigation of the deceptive act; and

(B) maintaining the action.

(b) The consumer protection division of the office of the attorney general shall use civil penalties collected under this article to enforce this article.